BUNDESREPUBLIK DEUTSCHLAND

CERTIFIED COPY OF PRIORITY DOCUMENT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	100 02 636.2
Anmeldetag:	21. Januar 2000
Anmelder/Inhaber:	Philips Corporate Intellectual Property GmbH, Aachen/DE
Bezeichnung:	Drahtloses Netzwerk mit einer Schlüsseländerungsprozedur
IPC:	H 01 Q, H 04 L, H 04 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 8. August 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Seiler

Seiler

A 9161
06/00
EDV-L

ZUSAMMENFASSUNG

Drahtloses Netzwerk mit einer Schlüsseländerungsprozedur

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten über Nutz- und Steuerkanäle und zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten dienen. Zu Beginn einer Schlüsseländerungsprozedur wird die Übertragung von Dateneinheiten angehalten. Die Funknetzwerk-Steuerung startet nach dem Austausch von Meldungen über den Zeitpunkt der Gültigkeit des neuen Schlüssels eine Prozedur zur Ermittlung, ob auch wenigstens ein Terminal den neuen Schlüssel verwendet. Nach der Prozedur wird die Übertragung von Dateneinheiten in Abhängigkeit von dem Prozedurergebnis mit dem neuen oder alten Schlüssel wieder aufgenommen.

Fig. 6

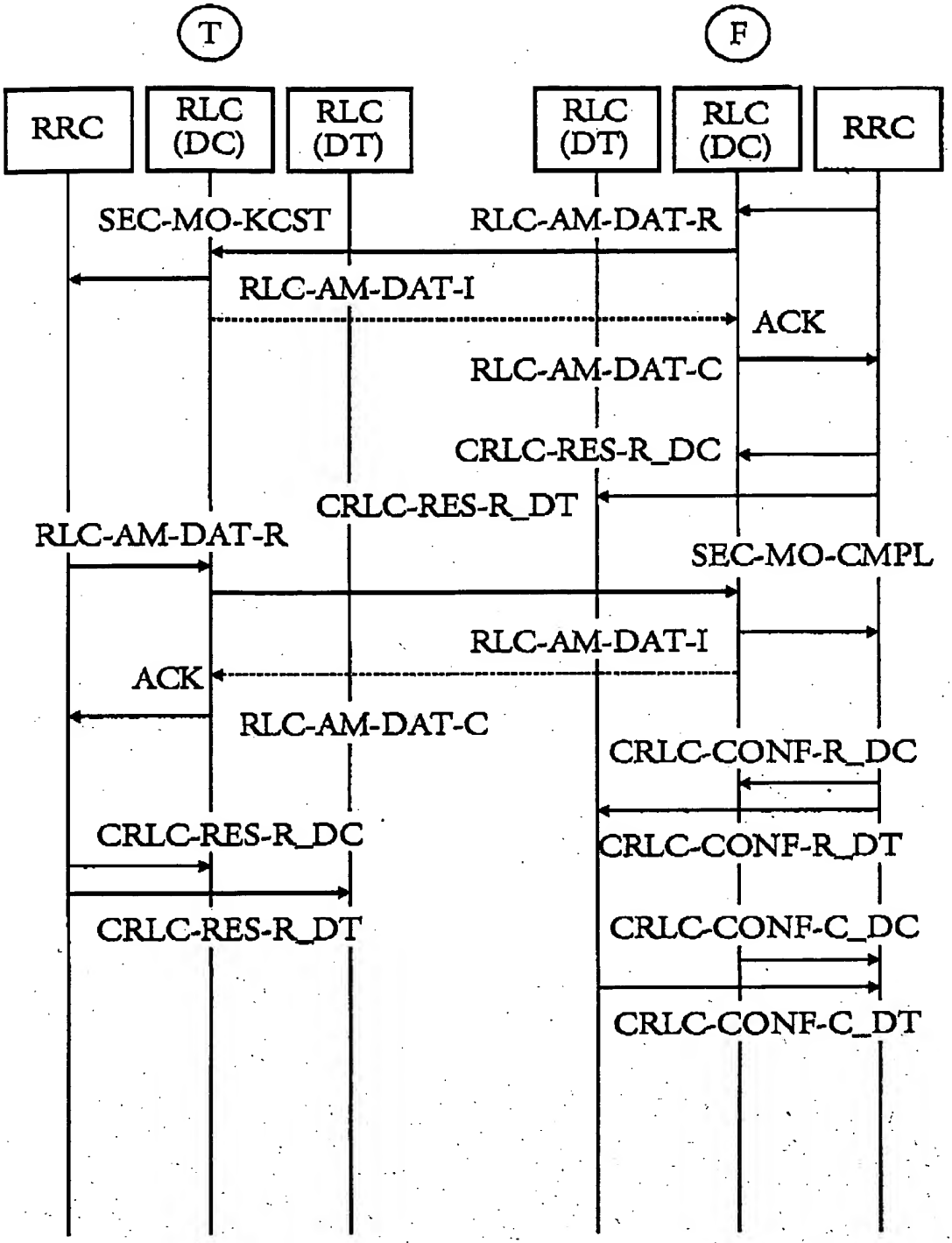

FIG. 6

PHDE000014

BESCHREIBUNG

Drahtloses Netzwerk mit einer Schlüsseländerungsprozedur

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals,

- die zur Verschlüsselung bestimmter zu übertragener Daten über Nutz- und Steuerkanäle,
- die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten und
- zu Beginn der Schlüsseländerung zum Anhalten der Übertragung von Dateneinheiten vorgesehen sind.

Aus dem Buch „The GSM System for Mobile Communications" von Michel Mouly und Marie-Bernadette Pautet, Verlag Cell & Sys, 1992, Seiten 391 bis 395, ist bekannt, dass Daten zwischen einer Basisstation und einem Terminal verschlüsselt übertragen werden. Der für die Übertragung benötigte Schlüssel wird in bestimmten Zeitabständen verändert. Hierfür ist eine Prozedur in drei Schritten vorgesehen.

Der Erfindung liegt die Aufgabe zugrunde, ein drahtloses Netzwerk zu schaffen, das eine andere Prozedur zur Änderung eines Schlüssels angibt.

Die Aufgabe wird durch ein drahtloses Netzwerk der eingangs genannten Art dadurch gelöst,
dass die Funknetzwerk-Steuerung nach dem Austausch von Meldungen über den Zeitpunkt der Gültigkeit des neuen Schlüssels zur Ermittlung vorgesehen ist, ob auch wenigstens ein Terminal den neuen Schlüssel verwendet, und nach der Überprüfung zum Aufnehmen der Übertragung von Dateneinheiten in Abhängigkeit von dem Überprüfungsergebnis mit dem neuen oder alten Schlüssel vorgesehen ist.

Unter dem erfindungsgemäßen drahtlosen Netzwerk ist ein Netzwerk mit mehreren Funkzellen zu verstehen, in denen jeweils eine Basisstation und mehrere Terminals Steuer-

und Nutzdaten drahtlos übertragen. Eine drahtlose Übertragung dient zur Übertragung von Informationen z.B. über Funk-, Ultraschall- oder Infrarotwege.

Erfindungsgemäß wird die Übertragung von Dateneinheiten zwischen wenigstens einem Terminal und der Funknetzwerk-Steuerung angehalten und dann überprüft ob ein Terminal und die Funknetzwerk-Steuerung denselben Schlüssel benutzen. Ist dies der Fall wird die Übertragung von Dateneinheiten mit dem neuen Schlüssel wieder aufgenommen. Im anderen Fall wird die Übertragung von Dateneinheiten mit dem alten Schlüssel fortgesetzt.

Ausführungsbeispiele der Erfindung werden nachstehend anhand der Fig. näher erläutert. Es zeigen:

Fig. 1	ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren Terminals,
Fig. 2	ein Schichtenmodell zur Erläuterung verschiedener Funktionen eines Terminals oder einer Funknetzwerk-Steuerung,
Fig. 3	ein Blockschaltbild zur Erläuterung des Verschlüsselungsmechanismus in einem Terminal oder einer Funknetzwerk-Steuerung und
Fig. 4 bis 7	Ablauf verschiedener Meldungen bei einer Schlüsseländerungsprozedur.

In Fig. 1 ist ein drahtloses Netzwerk, z.B. Funknetzwerk, mit einer Funknetzwerk-Steuerung (Radio Network Controller = RNC) 1 und mehreren Terminals 2 bis 9 dargestellt. Die Funknetzwerk-Steuerung 1 ist für Steuerung aller am Funkverkehr beteiligten Komponenten verantwortlich, wie z.B. der Terminals 2 bis 9. Ein Steuer- und Nutzdatenaustausch findet zumindest zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 statt. Die Funknetzwerk-Steuerung 1 baut jeweils eine Verbindung zur Übertragung von Nutzdaten auf.

In der Regel sind die Terminals 2 bis 9 Mobilstationen und die Funknetzwerk-Steuerung 1 ist fest installiert. Eine Funknetzwerk-Steuerung 1 kann gegebenenfalls aber auch beweglich bzw. mobil sein.

In dem drahtlosen Netzwerk werden beispielsweise Funksignale nach dem FDMA-, TDMA- oder CDMA-Verfahren (FDMA = frequency division multiplex access, TDMA = time division multiplex access, CDMA = code division multiplex access) oder nach einer Kombination der Verfahren übertragen.

Beim CDMA-Verfahren, das ein spezielles Code-Spreiz-Verfahren (code spreading) ist, wird eine von einem Anwender stammende Binärinformation (Datensignal) mit jeweils einer unterschiedlichen Codesequenz moduliert. Eine solche Codesequenz besteht aus einem pseudo-zufälligen Rechtecksignal (pseudo noise code), dessen Rate, auch Chiprate genannt, in der Regel wesentlich höher als die der Binärinformation ist. Die Dauer eines Rechteckimpulses des pseudo-zufälligen Rechtecksignals wird als Chipintervall T_C bezeichnet. $1/T_C$ ist die Chiprate. Die Multiplikation bzw. Modulation des Datensignals mit dem pseudo-zufälligen Rechtecksignal hat eine Spreizung des Spektrums um den Spreizungsfaktor $N_C = T/T_C$ zur Folge, wobei T die Dauer eines Rechteckimpulses des Datensignals ist.

Nutzdaten und Steuerdaten zwischen wenigstens einem Terminal (2 bis 9) und der Funknetzwerk-Steuerung 1 werden über von der Funknetzwerk-Steuerung 1 vorgegebene Kanäle übertragen. Ein Kanal ist durch einen Frequenzbereich, einen Zeitbereich und z.B. beim CDMA-Verfahren durch einen Spreizungscode bestimmt. Die Funkverbindung von der Funknetzwerk-Steuerung 1 zu den Terminals 2 bis 9 wird als Downlink und von den Terminals zur Basisstation als Uplink bezeichnet. Somit werden über Downlink-Kanäle Daten von der Basisstation zu den Terminals und über Uplink-Kanäle Daten von Terminals zur Basisstation gesendet.

Beispielsweise kann ein Downlink-Steuerkanal vorgesehen sein, der benutzt wird, um von der Funknetzwerk-Steuerung 1 Steuerdaten vor einem Verbindungsaufbau an alle Terminals 2 bis 9 zu verteilen. Ein solcher Kanal wird als Downlink-Verteil-Steuerkanal (broadcast control channel) bezeichnet. Zur Übertragung von Steuerdaten vor einem Verbindungsaufbau von einem Terminal 2 bis 9 zur Funknetzwerk-Steuerung 1 kann beispielsweise ein von der Funknetzwerk-Steuerung 1 zugewiesener Uplink-Steuerkanal

verwendet werden, auf den aber auch andere Terminals 2 bis 9 zugreifen können. Ein Uplink-Kanal, der von mehreren oder allen Terminals 2 bis 9 benutzt werden kann, wird als gemeinsamer Uplink-Kanal (common uplink channel) bezeichnet. Nach einem Verbindungsaufbau z.B. zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1 werden Nutzdaten über einen Downlink- und ein Uplink-Nutzkanal übertragen. Kanäle, die nur zwischen einem Sender und einem Empfänger aufgebaut werden, werden als dedizierte Kanäle bezeichnet. In der Regel ist ein Nutzkanal ein dedizierter Kanal, der von einem dedizierten Steuerkanal zur Übertragung von verbindungsspezifischen Steuerdaten begleitet werden kann. Zur Einbindung eines Terminals 2 bis 9 zu einer Funknetzwerk-Steuerung 1 ist ein kollisionsbehafteter Kanal mit wahlfreiem Zugriff zuständig.

Damit Nutzdaten zwischen der Funknetzwerk-Steuerung 1 und einem Terminal ausgetauscht werden können, ist es erforderlich, dass ein Terminal 2 bis 9 mit der Funknetzwerk-Steuerung 1 synchronisiert wird. Beispielsweise ist aus dem GSM-System (GSM = Global System for Mobile communication) bekannt, in welchem eine Kombination aus FDMA- und TDMA-Verfahren benutzt wird, dass nach der Bestimmung eines geeigneten Frequenzbereichs anhand vorgegebener Parameter die zeitliche Position eines Rahmens bestimmt wird (Rahmensynchronisation), mit dessen Hilfe die zeitliche Abfolge zur Übertragung von Daten erfolgt. Ein solcher Rahmen ist immer für die Datensynchronisation von Terminals und Basisstation bei TDMA-, FDMA- und CDMA-Verfahren notwendig. Ein solcher Rahmen kann verschiedene Unter- oder Subrahmen enthalten oder mit mehreren anderen aufeinanderfolgenden Rahmen einen Superrahmen bilden. Aus Vereinfachungsgründen wird im folgenden von einem Rahmen ausgegangen, der als Referenzrahmen bezeichnet wird.

Die Steuer- und Nutzdatenaustausch über die Funkschnittstelle zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 kann mit dem in Fig. 2 dargestellten, beispielhaften Schichtenmodell oder Protokollarchitektur (vgl. z.B. 3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) RAN; Working Group 2 (WG2); Radio Interface Protocol Architecture; TS 25.301 V3.2.0 (1999-10)) erläutert werden. Das Schichtenmodell besteht aus drei Protokollschichten: der physikalischen Schicht PHY, der Datenverbindungsschicht mit den Unterschichten MAC und RLC (in Fig. 2 sind mehrere

Ausprägungen der Unterschicht RLC dargestellt) und der Schicht RRC. Die Unterschicht MAC ist für die Medienzugriffssteuerung (Medium Access Control), die Unterschicht RLC für die Funkverbindungssteuerung (Radio Link Control) und die Schicht RRC für die Funkverwaltungssteuerung (Radio Resource Control) zuständig. Die Schicht RRC ist für die Signalisierung zwischen den Terminals 2 bis 9 und der Funknetzwerk-Steuerung 1 verantwortlich. Die Unterschicht RLC dient zur Steuerung einer Funkverbindung zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1. Die Schicht RRC steuert die Schichten MAC und PHY über Steuerungsverbindungen 10 und 11. Hiermit kann die Schicht RRC die Konfiguration der Schichten MAC und PHY steuern. Die physikalische Schicht PHY bietet der MAC-Schicht Transportverbindungen 12 an. Die MAC-Schicht stellt der RLC-Schicht logische Verbindungen 13 zur Verfügung. Die RLC-Schicht ist über Zugangspunkte 14 von Applikationen erreichbar.

Bei einem solchen drahtlosen Netzwerk werden die Daten aus Sicherheits- und Vertraulichkeitsgründen verschlüsselt über die Funkschnittstelle übertragen, um eine Abhören der Daten zu verhindern. Die Verschlüsselung wird in der Datenverbindungsschicht (z. B. in der RLC- oder MAC-Schicht) durchgeführt. Wie Fig. 3 zeigt, werden die Daten D über eine Exklusiv-Oder-Funktion (XOR) mit einer Verschlüsselungsmaske M verknüpft, so dass sich ein verschlüsselter Datenstrom C_D ergibt. Die Verschlüsselungsmaske M wird in einer Verschlüsselungs-Funktion 16 gebildet, die nach einem Verschlüsselungs-Algorithmus arbeitet und als Eingangswerte den Schlüssel CK und andere hier nicht näher dargestellte Parameter P erhält.

Der Schlüssel muss sowohl der Funknetzwerk-Steuerung 1 als auch den Terminals 2 bis 9 bekannt sein. Dieser Schlüssel wird zu bestimmten Zeitpunkten (z.B. alle 2 Stunden) mit einer speziellen Prozedur CKC (cipher key change) geändert, die als Schlüsseländerungs-Prozedur bezeichnet wird. Bei dieser Prozedur werden lokale Meldungen zwischen den Schichten RLC und RRC übertragen. In der Schicht RLC werden dabei noch Meldungen zwischen eigenen Instanzen RLC(DC) und RLC(DT) ausgetauscht. Die Instanz RLC(DT) ist für die Steuerung von dedizierten Nutzkanälen (dedicated traffic channel = DTCH) und die Instanz RLC(DC) für die Steuerung von dedizierten Steuerungskanälen (dedicated control channel = DCCH) zuständig.

Mit der Prozedur CKC wird von der Funknetzwerk-Steuerung 1 den Terminals 2 bis 9 der Zeitpunkt der Gültigkeit eines neuen Schlüssels mitgeteilt. Dieser neue Schlüssel ist sowohl der Funknetzwerk-Steuerung 1 als auch den Terminals 2 bis 9 bekannt. Die Fig. 4 bis 7 zeigen verschiedene Meldungen, die zwischen den Schichten RRC und RLC eines Terminals (linke Seite einer Fig. 4 bis 7, mit „T" angegeben) und der Funknetzwerk-Steuerung 1 (rechte Seite einer Fig. 4 bis 7, mit „F" angegeben) gesendet werden. Die folgenden Fig. 6 bzw. 7 beschreiben die Schlüsseländerungssprozedur CKC für den Fall, dass das Terminal den korrekten neuen Schlüssel verwendet bzw. dass das Terminal einen falschen neuen Schlüssel verwendet. Da vor dem endgültigen Umschalten auf Verschlüsselung und Entschlüsselung mit dem neuen Schlüssel erst noch überprüft wird, ob das Terminal den richtigen neuen Schlüssel verwendet, kann im Fehlerfall die Ver- und Entschlüsselung mit dem alten Schlüssel ohne den sonst resultierenden vollständigem Abbruch aller Verbindungen zwischen den Seiten T und F (datenverlustfrei) wieder fortgesetzt werden. In der nachfolgend beschriebenen Prozedur wird neben der Signalisierungsverbindung (DC) ein einziger dedizierter Nutzkanal betrachtet. Im allgemeinen Fall sind mehrere dedizierte Nutzkanäle und weitere dedizierte Steuerungskanäle (die nicht für die Signalisierungszwecke der Prozedur CKC verwendet werden) möglich, für die Prozedur entsprechend zu erweitern ist.

Die Prozedur CKC (Fig. 4) wird durch die lokalen Meldungen CRLC-S-R(ND_DC) bzw. CRLC-S-R(ND_DT) von der Schicht RRC der Seite F an die Instanzen RLC(DC) bzw. RLC(DT) angestoßen. Mit der Meldung CRLC-S-R(ND_DC) bzw. CRLC-S-R(ND_DT) wird der Instanz RLC(DC) bzw. RLC(DT) mitgeteilt, dass die Übertragung von Dateneinheiten angehalten werden soll, sofern die Folgenummer SN einer Dateneinheit (Jede Dateneinheit wird mit einer Folgenummer markiert) die Bedingung $SN \geq VTD\_DC + ND\_DC$ bzw. $SN \geq VTD\_DT + ND\_DT$ erfüllt. Dabei bedeutet der Parameter ND_DC bzw. ND_DT der lokalen Meldung CRLC-S-R(ND_DC) bzw. CRLC-S-R(ND_DT) eine Anzahl von noch zu übertragenden Dateneinheiten, und VTD_DC bzw. VTD_DT ist die in RLC(DC) bzw. RLC(DT) bekannte Folgenummer SN der nächsten erstmals zu sendenden Dateneinheit. Für den Steuerkanal DC ist ND_DC mindestens so groß zu wählen, dass alle Dateneinheiten der

nachfolgenden Downlink-Nachrichten SEC-MO-CMD und SEC-MO-KCST (Fig. 6 und 7) vor dem Anhalten der Übertragung noch geschickt werden können. Für den Nutzkanal kann ND_DT auch zu Null gesetzt werden.

Mit der lokalen Meldung CRLC-S-C(VTD_DC) bzw. CRLC-S-C(VTD_DT) bestätigt die Instanz RLC(DC) bzw. RLC(DT) der Seite F den Empfang der Nummer ND_DC bzw. ND_DT und gibt der Schicht die Nummer VTD_DC bzw. VTD_DT bekannt. Anschließend teilt die Schicht RRC der Seite F der Instanz RLC(DC) bzw. RLC(DT) über die Meldung CRLC-CONF-R_DC(CKN) bzw. CRLC-CONF-R_DT(CKN) den neuen zu verwendenden Schlüssel CKN mit. Diese Meldung wird von RLC(DC) bzw. RLC(DT) der Seite F mit der lokalen Meldung CRLC-CONF-C_DT bzw. CRLC-CONF-C_DC bestätigt.

Die Instanz RLC(DC) der Seite F sendet die in der lokalen Meldung RLC-DAT-R von der Schicht RRC erhaltene Nachricht SEC-MO-CMD an die Instanz RLC(DC) der Seite T (Terminal). Diese Nachricht stellt einen Befehl im Sicherheitsmode (security mode command) dar und wird mit dem alten, bisher gültigen Schlüssel verschlüsselt. In der Nachricht, die aus einer oder mehreren Dateneinheiten bestehen kann, sind die Nummern VTD_DC, ND_DC, VTD_DT und VTD_DT enthalten.

Nach Empfang dieser Nachricht zeigt die Instanz RLC(DC) der Schicht RRC der Seite T über die lokale Meldung RLC-AM-DAT-I an, dass diese Nachricht mit der Angabe angekommen ist, ab wann der neue Schlüssel gelten soll. Dieser neue Schlüssel gilt nämlich auf dem Steuerkanal DC für das Entschlüsseln ab der Folgenummer VTD_DC + ND_DC einer Dateneinheit und auf dem Nutzkanal ab der Folgenummer VTD_DT + ND_DT. Der Empfang der Nachricht SEC-MO-CMD in der Instanz RLC(DC) der Seite T wird über eine Empfangsbestätigung ACK der Instanz RLC(DC) der Seite F und weiter der Schicht RRC über die lokale Meldung RLC-AM-DAT-C bestätigt. Damit ist der Funknetzwerk-Steuerung 1 bekannt, dass das Terminal über den Beginn der Schlüsseländerungsprozedur informiert ist und den neuen Schlüssel zur Entschlüsselung von Dateneinheiten verwendet, deren Folgenummer SN die Bedingung SN ≥ VTD_DC + ND_DC im Falle des Steuerungskanals und SN ≥ VTD_DT + ND_DT im Falle eines Nutzkanals

erfüllt.

Mit den lokalen Meldungen CRLC-CONF-R_DC(CKN) bzw. CRLC-CONF-R_DT(CKN) instruiert nun die Schicht RRC der Seite F die Instanz RLC(DC), alle neuen, d.h. nicht als Wiederholung gesendeten, erwarteten Dateneinheiten (bis zur Vervollständigung der nächsten Nachricht) mit dem neuen Schlüssel zu entschlüsseln. Dies sind gerade die Dateneinheiten, für deren Folgenummer SN beim Empfang der gerade genannten lokalen Meldung CRLC-CONF-R_DC(CKN) bzw. CRLC-CONF-R_DT(CKN) die Bedingung SN ≥ VR erfüllt ist, wobei VR die in der Instanz RLC(DC) vorgehaltene Variable ist, welche die Folgenummer der nächsten, nicht als Wiederholung gesendeten, erwarteten Dateneinheit bedeutet.

Von der Seite T (Terminal) ausgehend (Fig. 5) wird ein ähnlicher Nachrichtenaustausch zwischen den betroffenen Schichten durchgeführt. Eine lokale Meldung CRLC-S-R(NU_DC) an die Instanz RLC(DC) bzw. CRLC-S-R(NU_DT) an die Instanz RLC(DT) von der Schicht RRC der Seite T startet den von der Seite T ausgehenden Nachrichtenaustausch. Mit diesen beiden lokalen Meldungen wird die Übertragung von Dateneinheiten angehalten, deren Nummer die Bedingung SN ≥ VTU_DC + NU_DC (für den Steuerkanal) bzw. SN ≥ VTU_DT + NU_DT (für den Nutzkanal) erfüllt, und der Instanz RLC(DC) bzw. RLC(DT) die Anzahl NU_DC bzw. NU_DT von noch zu übertragenen Dateneinheiten mitgeteilt. Für den Steuerkanal DC ist NU_DC (mindestens) so groß zu wählen, dass alle Dateneinheiten der nachfolgenden Uplink-Nachrichten SEC-MO-KC (Fig. 5) und SEC-MO-CMPL (Fig. 6 und 7) vor dem Anhalten der Übertragung noch geschickt werden können. Für den Nutzkanal kann NU_DT auch zu Null gesetzt werden.

Mit der lokalen Meldung CRLC-S-C(VTU_DC) bzw. CRLC-S-C(VTU_DT) bestätigt die Instanz RLC(DC) bzw. RLC(DT) der Seite T den Empfang der Nummer NU_DC bzw. NU_DT und gibt der Schicht die Nummer VTU_DC bzw. VTU_DT an. Diese Nummer VTU_DC bzw. VTU_DT gibt die Folgenummer SN der Dateneinheit an, die nach Empfang der lokalen Meldung CRLC-S-C(VTU_DC) bzw. CRLC-S-C(VTU_DT) auf dem Steuerkanal bzw. dem Nutzkanal im Uplink erstmals gesendet wird (also keine

wiederholte Übertragung). Anschließend teilt die Schicht RRC der Seite T den Instanzen RLC(DC) bzw. RLC(DT) einen Schlüsseländerungswunsch über die lokale Meldung CRLC-CONF-R_DC(CKN) bzw. CRLC-CONF-R_DT(CKN) mit. Mit den Nummern VTD_DC + ND_DC, VTD_DT + ND_DT wird außerdem diejenige Folgenummer von Dateneinheiten mitgeteilt, ab der mit dem neuen Schlüssel entschlüsselt werden sollen. Diese lokale Meldung wird von RLC(DC) und RLC(DT) der Seite T jeweils mit der lokalen Meldung CRLC-CONF-C_DC bzw. CRLC-CONF-C_DC bestätigt.

Mit der lokalen Meldung RLC-AM-DAT-R* von der Schicht RRC der Seite T an die Instanz RLC(DC) beginnt der Prozedurteil, mit dem die Seite F überprüfen kann, ob die Seite T den richtigen neuen Schlüssel benutzt. Nach dem Empfang der lokalen Meldung RLC-AM-DAT-R*, sendet die Instanz RLC(DC) der Seite T (Terminal) die Nachricht SEC-MO-KC an die Instanz RLC(DC) der Seite F (Funknetzwerk-Steuerung 1) verschlüsselt mit dem neuen Schlüssel. Der hochgesetzte Stern („*“) bedeutet, dass (z.B. durch einen zusätzlichen Parameter (Flag) in der lokalen Meldung RLC-AM-DAT-R) der Instanz RLC(DC) angezeigt wird, dass für diese spezielle Nachricht der neue Schlüssel zur Verschlüsselung verwendet werden soll.

Die Folgenummern der Dateneinheiten dieser Nachricht erfüllen in der Instanz RLC(DC) der Seite F die Bedingung SN ≥ VR, so dass sie mit dem neuen Schlüssel entschlüsselt werden. Die aus den Dateneinheiten, die mit dem neuen Schlüssel entschlüsselt wurden, wieder zusammengebaute Nachricht wird nun mit der lokalen Meldung RLC-AM-DAT-I* an die Schicht RRC der Seite F gegeben, wobei der hochgesetzte Stern („*“) bedeutet, dass (z.B. durch einen zusätzlichen Parameter (Flag) in der lokalen Meldung RLC-AM-DAT-I) der Schicht RRC angezeigt wird, dass die als Parameter übermittelte Nachricht aus Dateneinheiten zusammengebaut wurde, die mit dem neuen Schlüssel entschlüsselt wurden. Für eine sichere Überprüfung des korrekten Schlüssels kann es erforderlich sein, dass die Nachricht SEC-MO-KC aus mehreren Dateneinheiten besteht.

Die Schicht RRC der Seite F erwartet zu diesem Zeitpunkt genau die Nachricht SEC-MO-KC. Wird auf der Seite T der richtige neue Schlüssel zum Verschlüsseln verwendet, so erkennt die Schicht RRC im Parameter der lokalen Meldung

RLC-AM-DAT-I* diese Nachricht, und die Prozedur verläuft weiter wie in den Fig. 5 und 6 beschrieben.

Wird auf der Seite T ein falscher neuer Schlüssel zum Verschlüsseln verwendet, so erkennt die Schicht RRC im Parameter der lokalen Meldung RLC-AM-DAT-I* keine sinnvolle oder bekannte Nachricht. In diesem speziellen Fall, in dem eine unbekannte Nachricht mit der lokalen Meldung RLC-AM-DAT-I* von der Schicht RRC empfangen wurde, verwirft die Schicht RRC diese unbekannte Nachricht nicht einfach, sondern folgert, dass die Seite T einen falschen neuen Schlüssel verwendet. Die Prozedur setzt sich in diesem Falle, wie in Fig. 7 dargestellt, fort.

In beiden Fällen versendet die Schicht RRC der Seite F (als Parameter der lokalen Meldung RLC-AM-DAT-R an die Instanz RLC(DC)) an die Seite T die Nachricht SEC-MO-KCST, die einen Hinweis darüber enthält, ob die Schicht RRC der Seite F festgestellt hat, ob die Seite T den richtigen neuen Schlüssel verwendet oder einen falschen. Die Dateneinheiten der Nachricht SEC-MO-KCST werden immer mit dem alten Schlüssel verschlüsselt.

Im folgenden wird der in Fig. 6 gezeigte Normalfall beschrieben. Nach Empfang der lokalen Meldung RLC-AM-DAT-C, welche die Empfangsbestätigung ACK von RLC(DC) der Seite T für den Empfang der Nachricht SEC-MO-KCST der Seite F an die Schicht RLC(DC) der Seite F weiterreicht, instruiert die Schicht RRC der Seite F die Instanzen RLC(DC) und RLC(DT) mit der lokalen Meldung CRLC-RES-R_DC bzw. CRLC-RES-R_DT, die bisher angehaltenen Übertragungen von Dateneinheiten, deren Folgenummern SN in RLC(DC) die Bedingung $SN \geq VTD\_DC + ND\_DC$ bzw. in RLC(DT) die Bedingung $SN \geq VTD\_DT + ND\_DT$ erfüllen, wieder aufzunehmen. Diese Dateneinheiten werden mit dem neuen Schlüssel verschlüsselt.

Im folgenden wird der in Fig. 7 gezeigte Fehlerfall beschrieben. Nach Empfang der lokalen Meldung RLC-AM-DAT-C, welche die Empfangsbestätigung ACK von RLC(DC) der Seite T für den Empfang der Nachricht SEC-MO-KCST der Seite F an die Schicht RRC weiterreicht (vgl. Fig. 5), instruiert die Schicht RRC der Seite F nach weiter unter

beschriebenen ablaufenden Meldungen die Instanzen RLC(DC) und RLC(DT), zunächst mittels der lokalen Meldungen CRLC-CONF-R_DC bzw. CRLC-CONF-R_DT, bestätigt durch CRLC-CONF-C_DC bzw. CRLC-CONF-R_DT, die Umstellung auf den neuen Schlüssel rückgängig zu machen, und anschließend mit den lokalen Meldungen CRLC-RES-R_DC bzw. CRLC-RES-R_DT, die bisher angehaltenen Übertragungen von Dateneinheiten, deren Folgenummern SN in RLC(DC) die Bedingung SN ≥ VTD_DC + ND_DC bzw. in RLC(DT) die Bedingung SN ≥ VTD_DT + ND_DT erfüllen, wieder aufzunehmen. Diese Dateneinheiten werden mit dem alten Schlüssel verschlüsselt.

Durch die Empfangsbestätigung ACK wird der Seite T der Empfang der Nachricht SEC-MO-KC auf der Seite F bestätigt (Fig. 5). Die lokale Meldung RLC-AM-DAT-C gibt diese Bestätigung an die Schicht RRC auf der Seite T weiter. Nach Empfang dieser Bestätigung erwartet die Seite T die Nachricht SEC-MO-KCST von der Seite F (Fig. 6 und 7). Bei Empfang der Nachricht SEC-MO-KCST in der Instanz RLC(DC), deren Empfang wieder mit der Nachricht ACK der Seite F bestätigt wird, reicht diese Instanz der Seite T die Nachricht SEC-MO-KCST als Parameter der lokalen Meldung RLC-AM-DAT-I an die Schicht RRC der Seite T.

Wenn im Normalfall (Fig. 6) die Nachricht SEC-MO-KCST der Seite T anzeigt, dass der verwendete neue Schlüssel der richtige ist, versendet die Seite T die Nachricht SEC-MO-CMPL an die Seite F. Nach dem Empfang der lokalen Meldung RLC-AM-DAT-R (Fig. 6), sendet die Instanz RLC(DC) der Seite T (Terminal) die Nachricht SEC-MO-CMPL an die Instanz RLC(DC) der Seite F (Funknetzwerk-Steuerung). Diese Nachricht stellt einen Befehl im Sicherheitsmode (security mode complete) dar und wird mit dem alten, bisher gültigen Schlüssel verschlüsselt. Die Nachricht besteht aus einer oder mehreren Dateneinheiten und übermittelt die Nummern VTU_DC, NU_DC, VTU_DT und NU_DT. Nach Empfang dieser Nachricht zeigt die Instanz RLC(DC) der Schicht RRC der Seite F über die lokale Meldung RLC-AM-DAT-I an, dass diese Nachricht mit der Angabe angekommen ist, ab wann der neue Schlüssel zum Entschlüsseln in der Funknetzwerksteuerung gelten soll. Dieser neue Schlüssel gilt nämlich für Dateneinheiten, deren Folgenummer SN die Bedingung SN ≥ VTU_DC + NU_DC (Steuerkanal) bzw.

SN ≥ VTU_DT + NU_DT (Nutzkanal) erfüllt.

Nach Empfang der Nachricht SEC-MO-CMPL instruiert die Schicht RRC von F ihre Instanzen RLC(DC) und RLC(DT) mittels der lokalen Meldungen CRLC-CONF-R_DC bzw. CRLC-CONF-R_DT für das Entschlüsseln aller Dateneinheiten, deren Folgenummer SN die Bedingung SN ≥ VTU_DC + NU_DC in der Instanz RLC(DC) bzw. die Bedingung SN ≥ VTU_DT + NU_DT in der Instanz RLC(DT) erfüllt, den neuen Schlüssel zu verwenden. Damit endet die Prozedur CKC auf der Seite F im Normalfall.

Der Empfang der Nachricht SEC-MO-CMPL in der Instanz RLC(DC) der Seite F wird über die Empfangsbestätigung ACK der Instanz RLC(DC) der Seite T und weiter ihrer Schicht RRC über die lokale Meldung RLC-AM-DAT-C bestätigt. Damit ist dem Terminal bekannt, dass der Funknetzwerk-Steuerung 1 bekannt ist, dass das Terminal den neuen Schlüssel zum Verschlüsseln von Dateneinheiten eigener Nachrichten ab der Folgenummer VTU_DC + NU_DC auf dem Steuerkanal und VTU_DT + NU_DT auf dem Nutzkanal verwendet.

Da die Seite T den korrekten neuen Schlüssel verwendet, instruiert ihre Schicht RRC die Instanz RLC(DC) bzw. RLC(DT) nach Empfang der lokalen Meldung RLC-AM-DAT-C mit den lokalen Meldungen CRLC-RES-R_DC bzw. CRLC-RES-R_DT (Fig. 6) die bis dahin angehaltene Übertragung von Dateneinheiten wieder aufzunehmen, deren Folgenummern SN die Bedingung SN ≥ VTU_DC + NU_DC in der Instanz RLC(DC) für den Steuerkanal bzw. SN ≥ VTU_DT + NU_DT in der Instanz RLC(DT) für den Nutzkanal erfüllen. Diese Dateneinheiten werden mit dem neuen Schlüssel verschlüsselt. Damit endet die Prozedur CKC auf der Seite T im Normalfall.

Wenn die Nachricht SEC-MO-KCST der Seite T anzeigt, dass der verwendete neue Schlüssel ein falscher (Fehlerfall) ist (Fig. 7), instruiert ihre Schicht RRC die Instanzen RLC(DC) und RLC(DT) mittels der beiden lokalen Meldungen CRLC-CONF-R_DC bzw. CRLC_CONF-R_DT, die vorbereitete Umschaltung auf den neuen Schlüssel wieder

rückgängig zu machen.

Außerdem versendet die Seite T die Nachricht SEC-MO-CMPL an die Seite F, um die Prozedur zu beenden. Hierbei wird diese Nachricht als Parameter der lokalen Meldung RLC-AM-DAT-R an die Instanz RLC(DC) gegeben, über die Funkschnittstelle an die Instanz RLC(DC) der Seite F geschickt und von dieser als Parameter der lokalen Meldung RLC-AM-DAT-I der Schicht RRC der Seite F übergeben. Da kein Umschalten auf die Verwendung des neuen Schlüssels erfolgt, braucht die Nachricht SEC-MO-CMPL die Nummern VTU_DC, NU_DC, VTU_DT und NU_DT nicht zu enthalten. Die Dateneinheiten der Nachricht SEC-MO-CMPL werden ebenfalls mit dem alten Schlüssel verschlüsselt.

Da für das Entschlüsseln noch keinerlei Änderung in den Instanzen RLC(DC) bzw. RLC(DT) der Seite F erfolgt ist, ist auch keine Rekonfigurierung dieser Instanzen für das Entschlüsseln erforderlich, so dass die Prozedur CKC im Fehlerfall auf der Seite F mit dem Empfang der Nachricht SEC-MO-CMPL endet.

Nach Erhalt der Empfangsbestätigung ACK für die Nachricht SEC-M-CMPL der Schicht RLC(DC) der Seite T, wird diese an die Schicht RRC der Seite T durch die lokale Meldung RLC-AM-DAT-C weitergereicht. Die Schicht RRC der Seite T instruiert dann die Instanzen RLC(DC) und RLC(DT) mittels der beiden lokalen Meldungen CRLC-RES-C_DC bzw. CRLC-RES-C_DT die bis dahin angehaltene Übertragung von Dateneinheiten wieder aufzunehmen, deren Folgenummern SN die Bedingung $SN \geq VTU\_DC + NU\_DC$ in der Instanz RLC(DC) für den Steuerkanal bzw. $SN \geq VTU\_DT + NU\_DT$ in der Instanz RLC(DT) für den Nutzkanal erfüllen. Diese Dateneinheiten werden wegen der zuvor mittels der beiden lokalen Meldungen CRLC-CONF-R_DC in der Instanz RLC(DC) und CRLC-CONF-R_DT in der Instanz RLC(DT) rückgängig gemachten Umschaltung auf den neuen Schlüssel mit dem alten Schlüssel verschlüsselt. Damit endet im Fehlerfall die Prozedur CKC auf der Seite T.

PATENTANSPRÜCHE

1. Drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals,

- die zur Verschlüsselung bestimmter zu übertragener Daten über Nutz- und Steuerkanäle,
- die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten und
- zu Beginn der Schlüsseländerung zum Anhalten der Übertragung von Dateneinheiten vorgesehen sind,

dadurch gekennzeichnet,

dass die Funknetzwerk-Steuerung nach dem Austausch von Meldungen über den Zeitpunkt der Gültigkeit des neuen Schlüssels zur Ermittlung vorgesehen ist, ob auch wenigstens ein Terminal den neuen Schlüssel verwendet, und nach der Überprüfung zum Aufnehmen der Übertragung von Dateneinheiten in Abhängigkeit von dem Überprüfungsergebnis mit dem neuen oder alten Schlüssel vorgesehen ist.

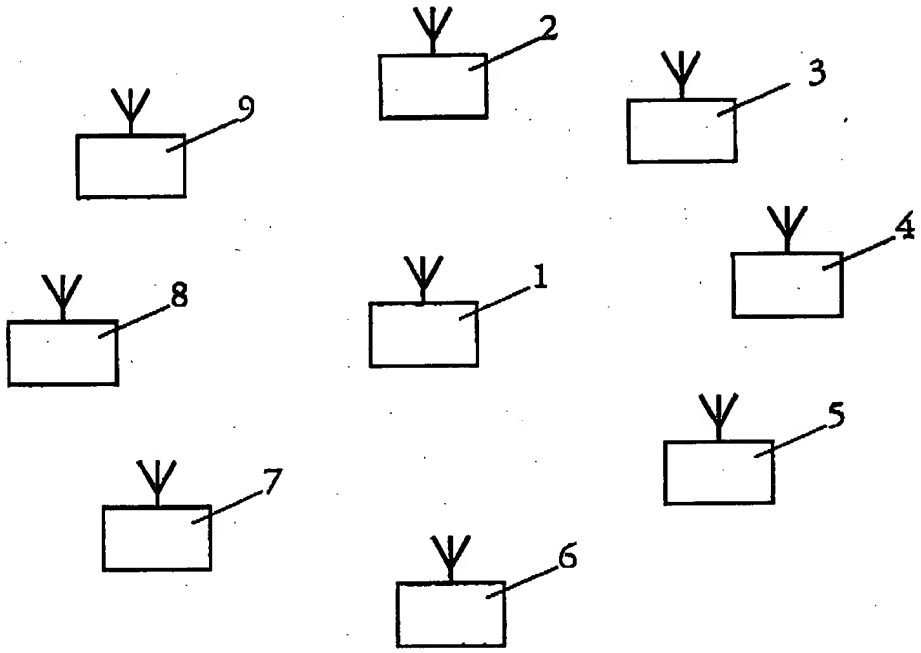

FIG. 1

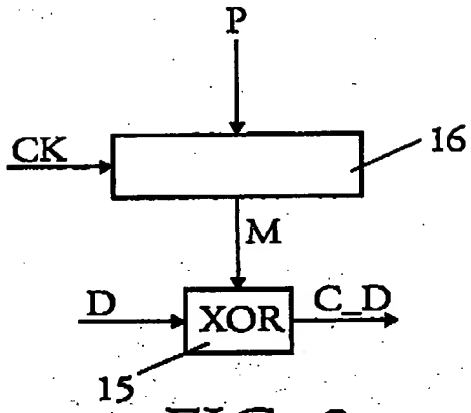

FIG. 3

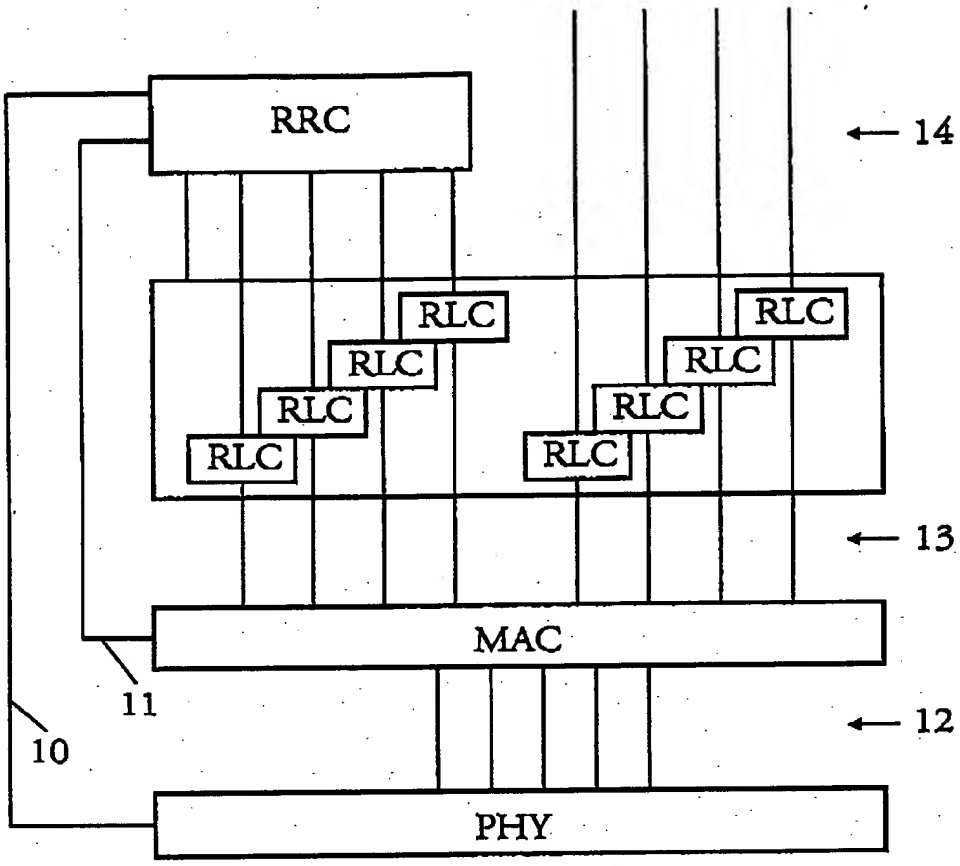

FIG. 2

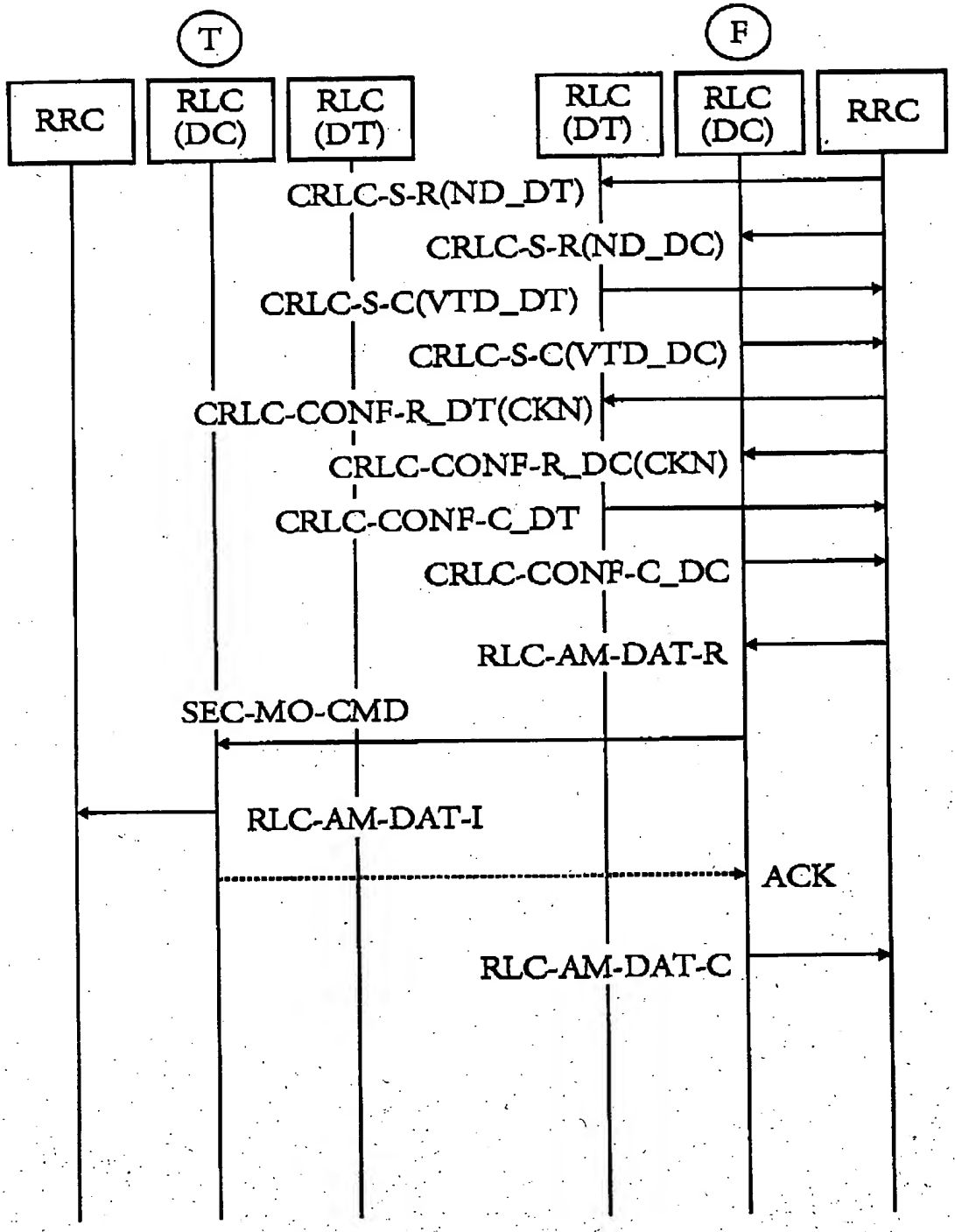
T
F
RRC
RLC (DC)
RLC (DT)
RLC (DT)
RLC (DC)
RRC
CRLC-S-R(ND_DT)
CRLC-S-R(ND_DC)
CRLC-S-C(VTD_DT)
CRLC-S-C(VTD_DC)
CRLC-CONF-R_DT(CKN)
CRLC-CONF-R_DC(CKN)
CRLC-CONF-C_DT
CRLC-CONF-C_DC
RLC-AM-DAT-R
SEC-MO-CMD
RLC-AM-DAT-I
ACK
RLC-AM-DAT-C

FIG. 4

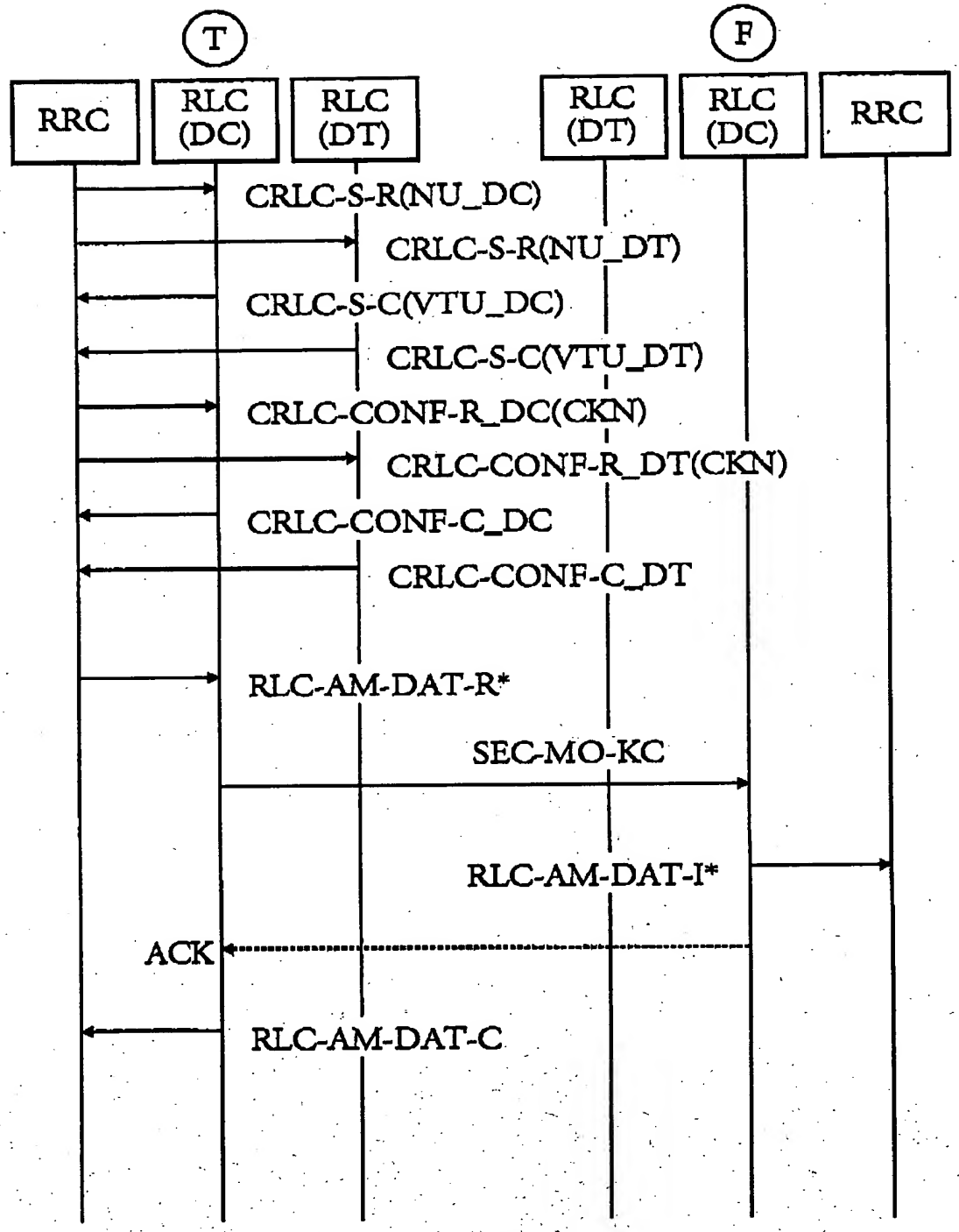

FIG. 5

4-VI-PHDE000014

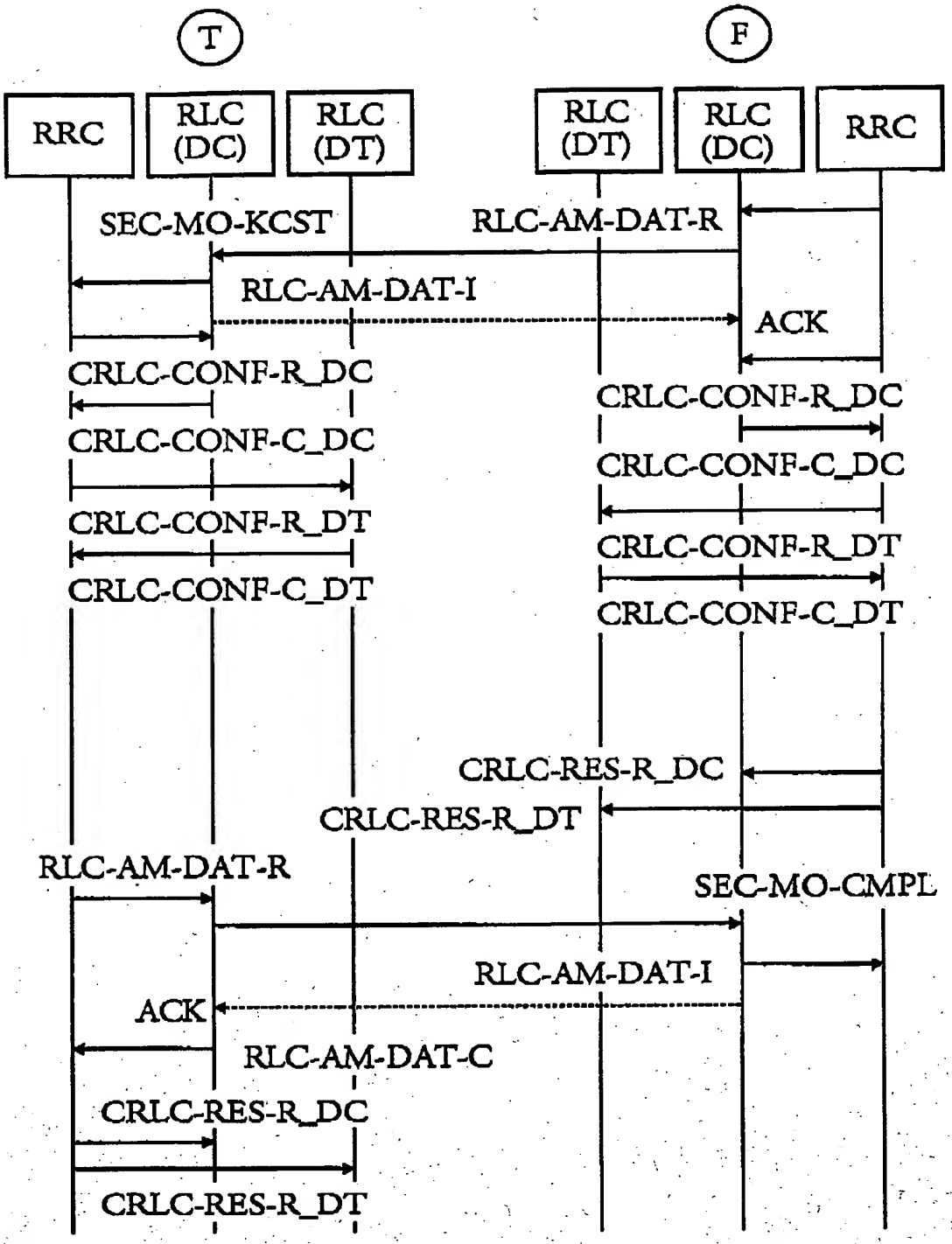

FIG. 7

6-VI-PHDE000014

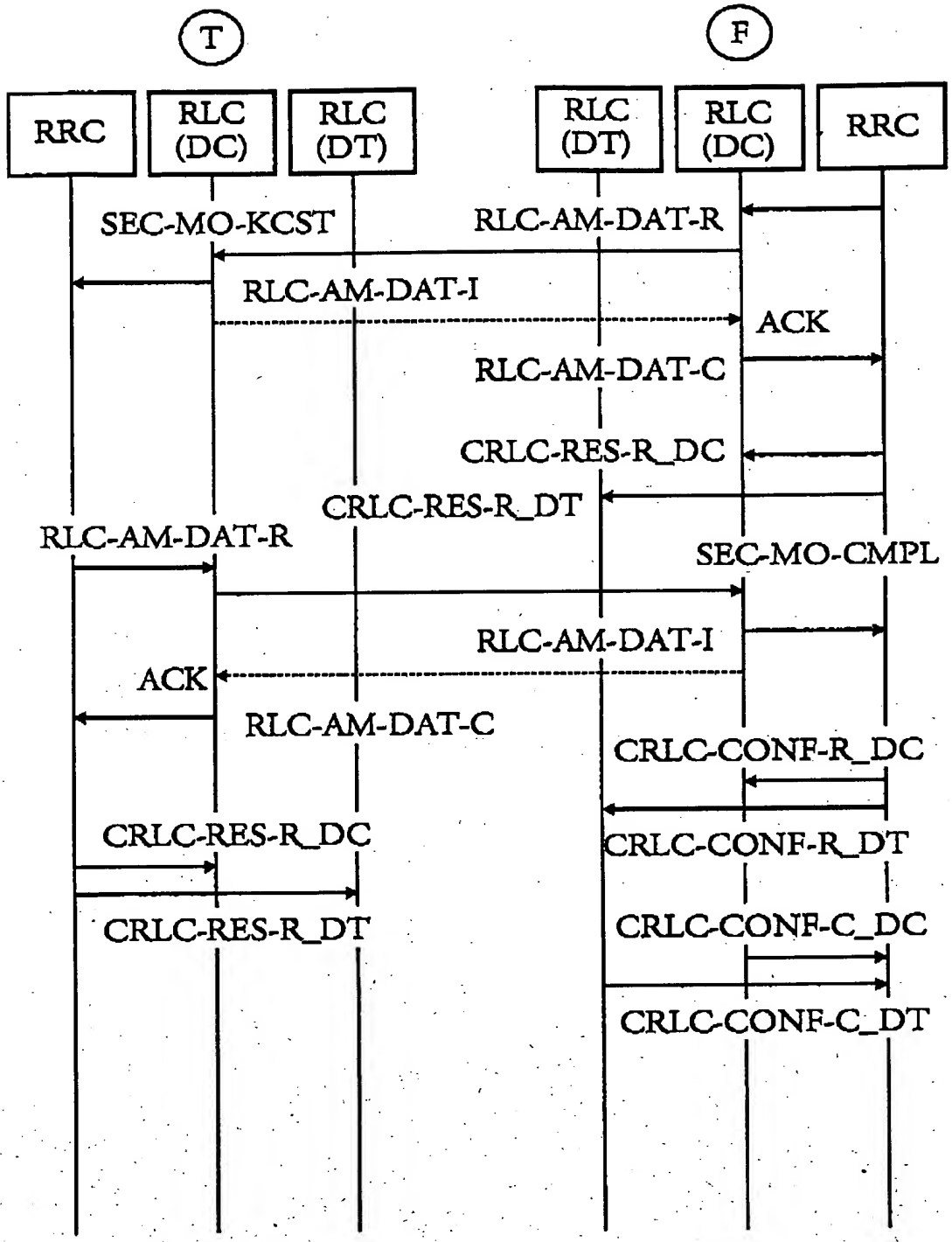

FIG. 6

5-VI-PHDE000014